Signal Authentication and Integrity Schemes for Next Generation Global Navigation Satellite Systems

Chris Wullems, Oscar Pozzobon, Kurt Kubik
Qascom S.r.l
Bassano del Grappa, Italy
{c.wullems, o.pozzobon}@qascom.com

Abstract
This paper describes a number of techniques for GNSS navigation message authentication. A detailed analysis of the security facilitated by navigation message authentication is given. The analysis takes into consideration the risk of critical applications that rely on GPS including transportation, finance and telecommunication networks. We propose a number of cryptographic authentication schemes for navigation data authentication. These authentication schemes provide authenticity and integrity of the navigation data to the receiver.

Through software simulation, the performance of the schemes is quantified. The use of software simulation enables the collection of authentication performance data of different data channels, and the impact of various schemes on the infrastructure and receiver. Navigation message authentication schemes have been simulated at the proposed data rates of Galileo and GPS services, for which the resulting performance data is presented.

This paper concludes by making recommendations for optimal implementation of navigation message authentication for Galileo and next generation GPS systems.

Introduction

Security services in GNSS can serve two purposes: First as a mitigation of the security vulnerabilities in GNSS and second as an application service.

- *Security for mitigation:* Security services can be used to provide a level of anti-spoofing for civil applications. This is particularly pertinent for applications that are safety or financially critical. Such critical applications range from tracking and timing applications to Safety of Life applications. An example of critical applications includes tracking of hazardous materials, power-phase synchronization, and transportation systems.
- *Security as a service:* Security can be used by applications as a service. An example of this is a scenario where legal traceability is needed. Security services could facilitate a method of providing location and time guarantees for a particular sequence of events, such as a car accident. In addition, security can be used to support applications such as secure time stamping and location-based access control.

The structure of this paper is as follows. First existing classes of security protection mechanisms suitable for GNSS are introduced. Security and operational aspects of these mechanisms are discussed, and an overview of next generation civil satellite navigation signals is given with a focus on the security protection mechanisms that are currently planned.

The paper then provides an in-depth analysis on Navigation Message Authentication (NMA) and introduces proposals for two NMA schemes. The schemes presented are based on signal and navigation message specifications for next generation GPS. Through our simulation tools, we are able to analyze the implementation possibilities on next generation GPS as an indicator as to what is possible for Galileo. Security and performance results of these schemes are discussed.

The paper concludes with a discussion of the applicability of these authentication schemes to Galileo, satellite and ground based augmentation systems.

Classes of Security Protection for GNSS

Security protection schemes for GNSS can be categorized into three classes:

Navigation Data Authentication and Cryptographic Integrity Protection Mechanisms
A navigation data authentication mechanism facilitates corroboration of the origin of data. Implicitly, this service provides data integrity, as unauthorized modification of a message results in a changed source of the data. Cryptographic integrity protection ensures information is not altered by unauthorized means by providing detection of such data manipulation.

Navigation Message Authentication (NMA) is one such mechanism designed to overcome spoofing and to provide increased safety and service guarantees. An NMA scheme would add authentication messages to the navigation message stream, both authenticating the source and providing cryptographic integrity protection of the navigation data.

Should an adversary attempt to generate or change the navigation data, a receiver would be able to detect the

activity. An adversary would not be able to simulate the authentication message, as he would not have the keys required to generate them.

Signal Access Control Mechanisms

A signal access control mechanism facilitates restriction of access to the signal from unauthorized users. GPS and Galileo signals use Direct Sequence Spread Spectrum (DSSS) and CDMA for both navigation function, through the pseudorange estimation process, and data modulation. Access to the signal can be restricted through Spreading Code Encryption (SCE), in which the secret spreading code is generated using a symmetric key and some type of stream-cipher. Only users with the key are able to generate the secret spreading code which then allows correlation and dispreading of the signal.

SCE can be used as a mitigation measure for spoofing or as a mechanism to support fee-paying services. Secure key distribution and management are particularly important in the use of SCE. Should the symmetric key be compromised, all users of the signal would require re-keying.

Asymmetric encryption methods and public key infrastructure (PKI) can be used to facilitate secure loading of keys, and electronic re-keying when required.

Navigation Data Access Control Mechanisms

A navigation data access control mechanism facilitates restriction of access to parts or all of a navigation data stream modulated over a given signal.

Navigation Data Encryption (NDE) can be used to support a variety of fee-paying value added services, or for example, to provide multiple levels of accuracy / availability, where non-encrypted navigation data such as ephemeris and clock correction terms are biased and corrections to the biased terms are given in an encrypted field which would accessed on a fee-paying basis.

Security Status of GNSS

This section provides a brief overview of the currently known status of civil signals in next generation satellite navigation systems and their support for security.

The next generation GPS will provide new civil services on the L2 and L5 frequencies. Table 1 lists the services, data rates and signals they operate on (Fontana et al. 2001) (Barker et al. 2000). No future civil services are currently projected to provide security protection mechanisms.

Signal	Data Modulated	SCE	Data Rate symbol/s (bit/s)	Service
$L1_Q$	Yes	No	50 (50)	L1 C/A
$L2_Q$	Yes	No	25 (50)	L2 Civil
$L5_I$	Yes	No	50 (100)	L5 Civil
$L5_Q$	No	No	--	L5 Civil

Table 1. New Civil GPS Signals

Galileo will provide four navigation services and one search and rescue service. A free of charge position and timing service will be broadcasted by the Open Service (OS). A guaranteed service providing timely warnings about the integrity will be implemented by the Safety of Life Service (SoL).

Two additional signals that allow service guarantee and increased accuracy, cryptographic integrity, a higher data rate throughput and limited broadcasting capacity will be provided by the Commercial Service (CS). Other two controlled access signals will provide position and timing to government controlled users in the Public Regulated Service (PRS) (Hein et al. 2002). Table 2 lists the security services projected to be included on each signal.

Signal	Data Mod	SCE	NMA	NDE	Data Rate Sym./s (bit/s)	Serv.
E2-L1-$E1_A$	Yes	Yes[2]	No	Yes	TBD (TBD)	PRS
E2-L1-$E1_B$	Yes	No	Yes[1]	CS Only	250 (125)	OS / SoL / CS
E2-L1-$E1_C$	Pilot	No	--	--	--	OS / SoL / CS
$E5a_I$	Yes	No	Yes[1]	No	50 (25)	OS / SoL
$E5a_Q$	Pilot	No	--	--	--	OS / SoL
$E5b_I$	Yes	No	Yes[1]	CS Only	250 (125)	OS / SoL / CS
$E5b_Q$	Pilot	No	--	--	--	OS / SoL / CS
$E6_A$	Yes	Yes[2]	No	Yes	TBD (TBD)	PRS
$E6_B$	Yes	Yes[3]	No	Yes	1000 (500)	CS
$E6_C$	Pilot	Yes[3]	--	--	--	CS

Table 2. GALILEO Signals

Navigation Message Authentication (NMA)

This section provides a detailed discussion of Navigation Message Authentication (NMA), the security protection afforded by its use, requirements for the development of NMA schemes and performance considerations.

A conceptual implementation of NMA is illustrated in Figure 1, in which both a simple and certified receiver are shown. A simple receiver would not offer any guarantee of service but would have full accuracy, simply ignoring the authentication messages. A certified

[1] Navigation Message Authentication may be included on the Open Service depending on feasibility analyses. (European Space Agency. (2002). "GALILEO Mission High Level Definition.")

[2] Government Spreading Code Encryption

[3] Commercial Spreading Code Encryption

receiver would contain the appropriate cryptographic algorithms to decode the authentication messages and verify the other messages in the stream.

Figure 1 illustrates the use of asymmetric encryption techniques for generating the authentication message, with a Public Key Infrastructure (PKI) supporting the NMA scheme.

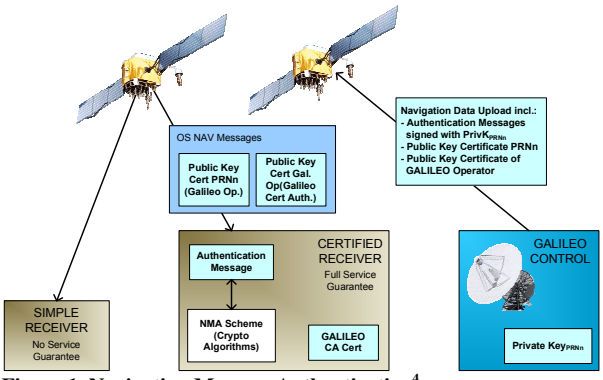

Figure 1. Navigation Message Authentication[4]

A public key certificate from the Galileo root Certification Authority (CA), pre-installed on the receiver, facilitates verification of the public key certificate of the Galileo operator subordinate CA which is broadcast to the receiver periodically with the public key certificate for each satellite.

The public key certificate for each satellite is issued by the Galileo operator CA, certifying the satellite's public key. The receiver is able to verify the public key and corresponding private key used to generate the authentication messages are in fact from the Galileo operator and not an adversary attempting to generate authentication messages with keys they have generated. A more in-depth discussion on PKI is given later in this paper.

Security protection afforded by NMA

NMA provides data-level anti-spoofing functionality through the use of authentication messages, which provide origin authentication and cryptographic integrity of the navigation message stream. NMA significantly increases the complexity of spoofing a legitimate signal through simulation, however, it has a security limitation in that the messages could theoretically be acquired by a receiver and modulated over a simulated signal in order to spoof the Galileo signal.

This would require functionality that is not commonly found in commercial signal simulators, and would require the operation to be performed within a very small time window. This type of attack would require significant cost in terms of engineering skills and equipment. We are currently working on mitigation strategies that address this problem, and are confident in achieving a high-level of anti-spoofing protection for civil receivers.

NMA Requirements

GNSS data channels are characteristically slow to ensure optimum navigation performance. This and the need for optimum alert times for integrity failure, result in a number of requirements for an NMA scheme on GNSS as given below:

- *Efficient verification:* As GNSS receivers may have limited computational power, the overhead for verification of the authentication message should be low;
- *Fast authentication:* In order to maintain a low time-to-alert of integrity / authentication failure, it is imperative that the authentication is fast and as close to real-time as possible;
- *Loss-tolerance:* Robustness of the authentication scheme to message loss is critical in order to maintain high time-to-alert rates. This is particularly pertinent in the case of GNSS, which broadcasts the navigation data. In the case of data corruption or loss, a receiver must wait till the message is next transmitted. Mechanisms such as Forward Error Correction (FEC) and Cyclic Redundancy Checks (CRC) assist in reducing data corruption and loss;
- *Scalability:* Scalability is a key requirement for authentication in GNSS. The number of receivers should be independent of the authentication scheme. In addition, the key distribution mechanisms used should be scalable; and
- *Low Communications Overhead:* As data channels in GPS/Galileo have very limited bandwidth, the authentication scheme must be very efficient in terms of communications overhead.

NMA Performance Considerations

There are a number of considerations that must be addressed in an NMA scheme. In particular, the performance of satellite navigation systems, in terms of delays for broadcasting ephemeris and clock correction terms, must be balanced with the need and desired performance levels for authentication.

The Galileo Mission High-Level Definition (European Space Agency 2002) states:

> "Capability to authenticate the signal (e.g. by a digital signature) must be transparent and non-discriminatory to users and shall not introduce any degradation in performances."

A balance must be obtained where NMA performance is sufficient without resulting in degradation in performance. Table 3 details the maximum broadcast

[4] Figure based on concepts from Galilei Consortium. (2003). "The Galilei Project: GALILEO Design Consolidation."

intervals for various CNAV messages on the GPS L2C signal. As Galileo navigation message are yet to be defined, there is currently no performance data available.

Message Data	Message Type Number	Maximum Broadcast Intervals
Ephemeris	10 & 11	48 sec
Clock	Type 30's	48 sec
ISC, IONO	30[5]	288 sec
Reduced Almanac	31[5] or 12	20 min[6]
Midi Almanac	37[5]	120 min[6]
EOP	32[5]	30 min
UTC	33[5]	288 sec
Diff Correction	34[5] or 13 & 14	30 min[7]
GGTO	35[5]	288 sec
Text	36[5] or 15	As required

Table 3. Maximum CNAV Message Broadcast Intervals (ARINC Engineering 2004).

Depending on the performance of the NMA schemes, the time-to-alarm for authentication / integrity failure may be outside the time-to-alarm requirements of some Safety of Life (SoL) applications for non-intentional integrity failures. For example, GPS used in time-critical applications would be more sensitive to long time-to-alert periods than applications such as hazardous materials tracking or secure time stamping.

Integrity performance requirements for the Safety of Life Service (SoL) service are detailed in Table 4. These requirements were derived from service levels that are stipulated by law or are recommended best practices for all considered domains of transportation e.g. aviation, maritime and rail (European Space Agency 2002).

SoL Integrity Service Level	A	B	C
Coverage	World Land Masses	Global	Global
Alarm Limit	H: 40m V: 20m	H: 556m V: -m	H: 25m V: -m
Time-To-Alarm	6s	10s	10s
Integrity Risk	3.5×10^{-7}/ 150s period	10^{-7}/ 1hr period	10^{-5}/ 1hr period
Continuity Risk	8×10^{-6}/ 15s period	(TBD)/ 1hr period	3×10^{-4}/ 3hr period
Availability	99.5%	99.5%	99.5%
Applications	Aviation, APV II, Road, Rail	Aviation en-route to NPA	Maritime

Table 4. GALILEO Safety of Life Service Characteristics (Galilei Consortium 2003)

[5] Type 30 messages contain clock correction parameters.

[6] Maximum broadcast interval for a complete set of SVs in the constellation.

[7] Only applicable when differential corrections are available.

Integrity in this context is defined to be the ability of a system to provide timely warnings to the user when it fails to meet certain margins of accuracy. SoL data including integrity and Signal in Space Accuracy (SISA) aim to facilitate the required time-to-alarms in Table 4.

It is our belief that some SoL applications may additionally require equivalent time-to-alarms for authentication / cryptographic integrity failure caused by intentional interference such as spoofing. Such intentional interference could be potentially disastrous in safety critical applications.

Proposed Authentication Schemes

This section discusses the assumptions, message configuration and Public Key Infrastructure (PKI) used in the proposals and the corresponding performance analyses.

In the absence of a NAV message structure and indications of the required broadcast intervals, we have designed the schemes around the CNAV navigation message structure for the GPS L2C signal.

A CNAV message is a 300 bit message composed of a 38 bit header containing the satellite PRN ID, a message ID, the Time of Week (TOW) and an alert flag to indicate that the User Range Accuracy (URA) may be worse than indicated. CNAV messages also contain a 24 bit Cyclic Redundancy Check (CRC) (ARINC Engineering 2004). (Refer to Figure 2)

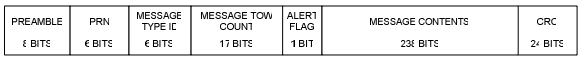

Figure 2. GPS L2C CNAV Message

CNAV messages can be sequenced in 36 second[8] sequences of three messages or 48 second sequence of four messages. Only these sequencing options provide performance that meets the maximum broadcast intervals of navigation data required for the GPS L2C. (Refer to Table 3 for maximum broadcast intervals)

The sequencing of navigation messages is arbitrary, but broadcast for optimal performance. The 48 second sequence offers the best performance for NMA. Figure 3 illustrates the 48 second message sequence, in which type 10 and 11 ephemeris messages are required to be broadcast every sequence in order to meet the maximum broadcast interval requirements, allowing two messages allocations for the scheduling of the other messages including the proposed authentication messages.

[8] Based on the bit rate of the GPS L2C data channel.

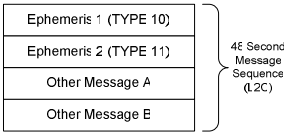

Figure 3. CNAV Message Sequence of 48 Seconds (L2C)

Qascom has developed a GNSS security simulator for simulation of NMA for various message structures and phasing configurations. The CNAV structure defined for performance analysis of the NMA schemes is based on the IS-GPS-200 Interface Specification (ARINC Engineering 2004). An example message phasing configuration is illustrated in Figure 4, where message type 60 and 61 are the two messages used for NMA.

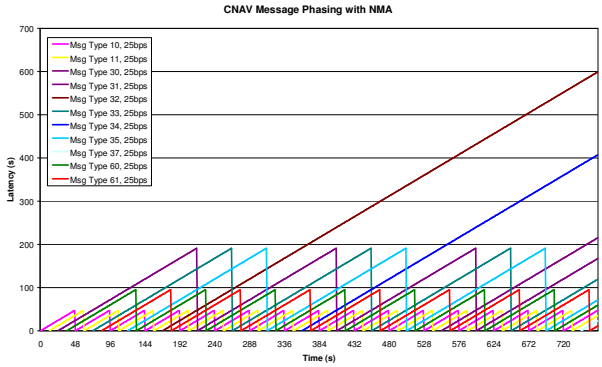

Figure 4. CNAV Message Phasing with NMA

Public Key Infrastructure

Public key infrastructure (PKI) is integral in providing a framework for distribution of public keys in a trusted way. The operational environment of a GNSS PKI is unique, in that all communication to the receiver is via broadcast data channels. Revocation has to be handled differently from standard PKIs, as it has to be assumed that the receiver has no access to on-line certificate revocation information.

Revocation could be facilitated through an alert flag in the authentication message, indicating that the receiver must obtain a new operator certificate before it can continue to verify the cryptographic integrity of navigation messages.

An example model of a GNSS PKI is illustrated in Figure 5. A certified receiver must have the Galileo CA certificate pre-installed, hypothetically by the receiver manufacturer. The Galileo operator certificate would be broadcast in the navigation message stream, such that the receiver is able to verify the operator CA certificate using the Galileo CA certificate.

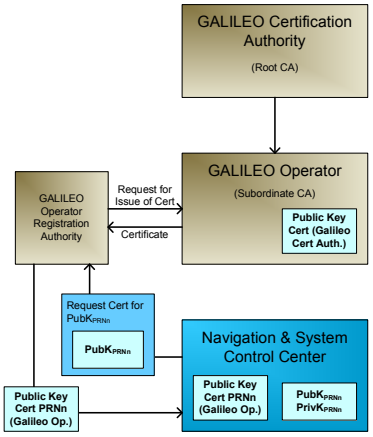

Figure 5. Example Public Key Infrastructure

The use of a subordinate CA allows for periodic re-keying of the satellites, and supports revocation and issue of new operator CA certificates.

Table 5 and Table 6 illustrate binary certificates based on X.509 optimized for transmission in CNAV messages. The key sizes are based on the use of Elliptic Curve Cryptography, and a selection of curves that is considered safe by the National Institute for Standards and Technology (NIST) (NIST 1999).

Certificate Field	Size (bits)
Serial Number	32
Valid From	32
Valid To	32
Issuer	192
Satellite PRN ID	6
Satellite Public Key	163
Operation Center CA Signature Algorithm[9]	6
Operation Center CA Signature	566

Table 5. Binary Satellite Certificate Format for CNAV

Certificate Field	Size (bits)
Serial Number	32
Valid From	32
Valid To	32
Issuer	192
Subject (Operator)	192
Operator Public Key	283
CA Signature Algorithm[9]	6
CA Signature	566

Table 6. Binary Operator CA Certificate Format for CNAV

[9] These bits define the algorithm type and the elliptic curve to be used.

NMA using EC-DSA Signature Scheme

A Navigation Message Authentication scheme based on concepts from the Galilei project design consolidation (Galilei Consortium 2003) is discussed in this section.

The authentication scheme is based on the broadcast of digital signatures of sequences of messages. Elliptic Curve Digital Signature Algorithm (EC-DSA) was chosen for this implementation due to the small key and digital signature sizes.

The message structure for this scheme is illustrated in Figure 6, where *A* denotes a satellite.

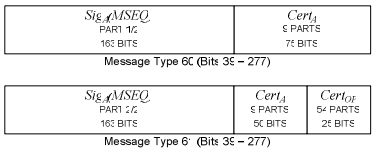

Figure 6. Message Structure

In a given timeslot of 96 seconds, a signature of two sequences of messages except type 60 and 61 messages is calculated. The signature, $Sig_A(MSEQ)$, and public key certificates of *A* and the operator, are broadcast in type 60 and 61 messages. These messages are broadcast alternately in each message sequence, such that in a given timeslot, both message types 60 and 61 are received.

It is assumed that $Cert_A$ is issued by a Certification Authority (CA), such as the Galileo Operator CA. The operator certificate is transmitted in 54 packets of 25 bits. Each satellite transmits from a different index in the set of 54 packets, such that time to acquire all parts is reduced significantly as the parts and be acquired from all visible satellites.

The receiver must only accept $Sig_A(MSEQ)$ if it is able to verify the public key of *A* and $Sig_A(MSEQ)$ is successfully verified.

Performance

This scheme was simulated with the security simulator developed by Qascom. A summary of the key performance indicators are detailed in Table 7. As can be seen by these results, the time-to-alarms for cryptographic integrity failure are outside all time-to-alarm requirements for class A, B and C SoL applications. (Refer to Table 4)

	GPS L2C (25 bps)	**GPS L5 (50 bps)**	**Galileo OS E2-L1-E1$_B$ (125 bps)**	**Galileo OS E5A$_I$ (25 bps)**	**Galileo OS E6B$_I$ (125 bps)**
Time-To-Alarm	96s	48s	19,2s	96s	19,2s
Cert Acquisition Time (PRNn Cert)	864s	432s	172,8s	864s	172,8s
Cert Acquisition Time (Operator) [10]	840s	420s	168s	840s	168s

Table 7. Performance of NMA using Digital Signatures

Security of the Scheme

The strength of a particular signature depends on all the links in the security chain. This includes the signature and hash algorithms used, as well as the strength of key generation. In particular, the security of EC-DSA requires the careful selection of both key sizes and elliptic curve domain parameters. The parameters and key sizes chosen in the design of this scheme are recommended curves that are considered safe by the National Institute for Standards and Technology (NIST) (NIST 1999).

A further consideration of security in this scheme is the possibility of an adversary to forge signatures. Given enough messages and corresponding signatures it may be possible deduce a pattern and then forge a signature of choice. While in practice this may not be feasible, it is prudent to design the scheme such that the validity of the operator's public key certificate is relatively short. This would require periodic generation of new keys for each satellite and recertification of the satellites' public keys by the operator CA.

NMA using Proposed Scheme based on TESLA

In this section we present a proposed NMA scheme based on a modified version of the Time Efficient Stream Loss Tolerant Authentication (TESLA) protocol (Perrig et al. 2002). TESLA uses Message Authentication Codes (MAC) to achieve cryptographic integrity of broadcast messages.

The advantage of using MACs is the reduction in computation and communications overhead compared to the use of asymmetric cryptography. It is additionally scalable to a large number of receivers, supporting most of the NMA requirements previously discussed. The modification we have introduced is the synchronization system.

[10] Value is based on reception of packets from 6 satellites.

This protocol can support numerous configuration options that allow for optimization for certain services and required quality of service guarantees.

Synchronization

As the TESLA protocol is based on a delayed key release scheme, time synchronization is critical and directly affects the security of the scheme. We propose a synchronization scheme based on the Time of Week (TOW) field in the CNAV message header (Refer to Figure 2).

The TOW value is the 17 Most Significant Bits (MSB) of the 19 Least Significant Bits (LSB) of the 29 bit Z-COUNT. In each GPS Satellite Vehicle (SV) the X1 epochs of the P-Code are used for precise counting and communicating time. The Z-COUNT increments in X1 epochs (1,5 seconds), the 19 LSBs of which indicate the number of X1 epochs that have occurred since the transition from the previous week. The 10 MSBs of the Z-COUNT indicate the current GPS week.

The value of the TOW count in the CNAV message header multiplied by 6 represents the SV time in seconds at the start of the next 12-second CNAV message (ARINC Engineering 2004).

For synchronization of the NMA scheme, we define the following counters:[11]

$$AUTHCOUNT = floor\left(\frac{TOW}{16}\right) = \langle 0 \ldots 6299 \rangle$$

$$TIMESLOT = AUTHCOUNT \bmod 300 = \langle 0 \ldots 299 \rangle$$

The duration of a timeslot is 96 seconds, two CNAV message sequences. The timing relationships are illustrated in Figure 7.

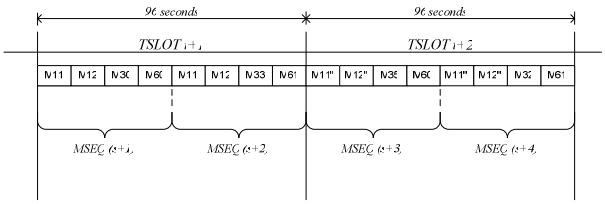

Figure 7. Synchronization of Proposed Authentication Scheme

Scheme Setup and Broadcast

The following initialization procedure is used to setup a hash chain, such that there is a hash value K_n for every 96 seconds for 300 timeslots. A hash chain of 300 values lasts for 8 hours.

[11] The function *floor(x)* rounds *x* to the nearest integer less than or equal to *x*.

A is defined to be satellite PRN ID *n*
B is defined to be a GPS receiver

1. *A* computes $K_{300} = F(s)$, where *s* is a random secret number chosen by *A*
2. *A* computes K_0 by hashing K_{300} 300 times, such that $K_{299}=F(K_{300})$, $K_{298}=F(K_{299})$,… $K_0=F(K_1)$. The values $K_{299} \ldots K_0$ are kept secret.
3. $A \rightarrow B$: $Sig_A(K_0)$, K_0, $Cert_A$

It is assumed that $Cert_A$ is issued by a Certification Authority (CA), such as the Galileo Operator CA. The receiver must only accept K_0 if it is able to verify the public key of *A* and $Sig_A(K_0)$ is successfully verified.

A key disclosure delay of one timeslot is used, such that within a given timeslot, key K_{n+1} is released in message type 60 with the MAC of the message sequence. The MAC is keyed with K'_{n+2} and is calculated over all messages except type 60 and 61. $Sig_A(K_0)$ and the public key certificates for the satellite and operator are included in message type 61. Refer to Figure 7 and Figure 8 for illustration of the timing relationships of these messages and the generation of type 60 and 61 authentication messages.

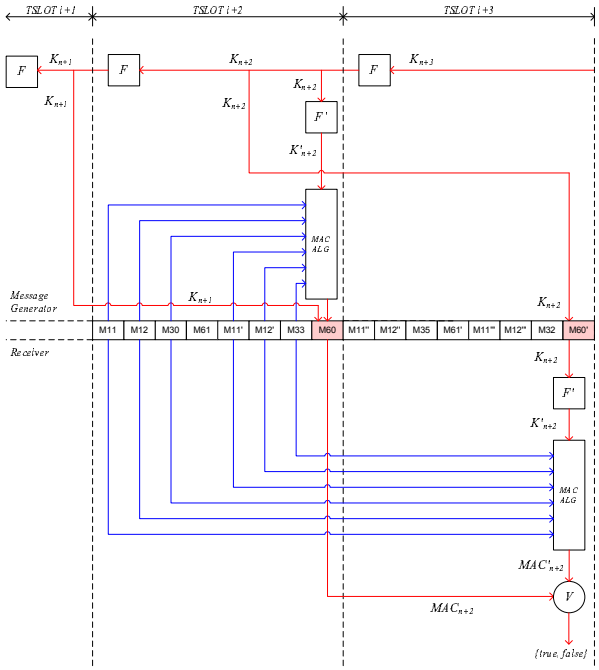

Figure 8. Authentication Message Generation and Verification Process

The structures of the type 60 and 61 messages are illustrated in Figure 9.

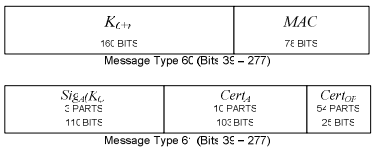

Figure 9. Message Structure

Authentication and Integrity Verification Process

This subsection describes the authentication and integrity verification process. It is assumed that the receiver has already obtained K_0 from a series of type 61 messages. Figure 8 illustrates the generation and verification of authentication messages.

In the following example, the receiver starts receiving messages in timeslot *i+2*.

F(x) is defined to be a secure hash function
F'(x) is defined to be a secure key generation function
MAC denotes a message authentication code

<u>*TIMESLOT i+2*</u>
Received Messages:
$\{M_{11},M_{12},M_{30},M_{60},M_{11}',M_{12}'M_{33},M_{61}\}$

1. Obtain K_{n+1} from M_{60}
2. Receiver calculates $Kv_{n+1} = F(K_n)$. If receiver does not have K_n, must verify chain back to K_0 such that $Kv_{n+1} = F(F(..(F(K_0)))$
3. K_{n+1} is authenticated if $Kv_{n+1} = K_{n+1}$
4. No verification is possible at this stage as key K_{n+2} has not yet been released and $MAC(K'_{n+2})\{M_{11},M_{12},M_{30},M_{11}',M_{12}'M_{33}\}$ cannot be calculated.

<u>*TIMESLOT i+3*</u>
Received Messages:
$\{M_{11}'',M_{12}'',M_{35},M_{60}',M_{11}''',M_{12}'''M_{32},M_{61}'\}$

1. Obtain K_{n+2} from M_{60}'
2. Receiver calculates $Kv_{n+2} = F(K_{n+1})$
3. K_{n+2} is authenticated if $Kv_{n+2} = K_{n+2}$
4. Receiver generates key K'_{n+2} from K_{n+2} using key generation algorithm *F'(x)* such that $K'_{n+2} = F'(K_{n+2})$
5. Obtain $MAC(K'_{n+2})$ from M_{60}'
6. Receiver calculates $MACv(K'_{n+2})\{M_{11},M_{12},M_{30},M_{11}',M_{12}'M_{33}\}$
7. Integrity of messages in *TIMESLOT i+2* is verified if $MACv(K'_{n+2}) = MAC(K'_{n+2})$

Alternate Message Configurations

This subsection proposes an alternate message configuration more suitable to higher-rate channels in Galileo, facilitating faster time-to-alert. Assuming a navigation message structure similar to CNAV, and the same maximum broadcast intervals for ephemeris and clock correction terms, many more messages could be interleaved in the message sequence without affecting the minimum broadcast intervals.

The type 60 message would be included in every message sequence of four messages. The type 61 message containing $Sig_A(K_0)$, $Cert_A$, and $Cert_{OP}$ would be interleaved in the remaining sequenced messages for best performance.

As a new hash value K_{0+n} would be released every 48 seconds instead of every 96 seconds, the *AUTHCOUNT* and *TIMESLOTS* are redefined as follows:

$$AUTHCOUNT = floor\left(\frac{TOW}{8}\right) = \langle 0 \ldots 12599 \rangle$$

$$TIMESLOT = AUTHCOUNT \bmod 600 = \langle 0 \ldots 599 \rangle$$

Figure 10 illustrates the timing relationships for synchronization in 48 second timeslots.

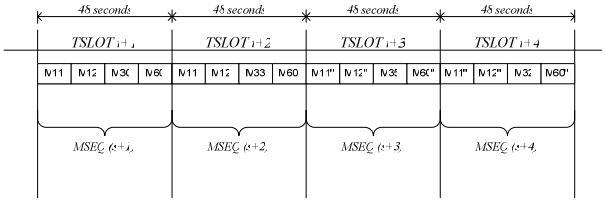

Figure 10. Synchronization with Message Configuration 2

Performance

This scheme was simulated with the security simulator developed by Qascom. The values in Table 8 and Table 9 for Galileo services are indicators of time-to-alarms if a CNAV type structure is adopted.

A summary of the key performance indicators for message configuration 1 are detailed in Table 8. As can be seen by these results, the time-to-alarms for cryptographic integrity failure are outside all time-to-alarm requirements for class A, B and C SoL applications (Refer to Table 4).

	GPS L2C (25 bps)	GPS L5 (50 bps)	Galileo OS E2-L1-E1$_B$ (125 bps)	Galileo OS E5A$_I$ (25 bps)	Galileo OS E6B$_I$ (125 bps)
Time-To-Alarm	96s	48s	19,2s	96s	19,2s
Signature of K_0 for a given hash chain	288s	144s	57,6s	288s	57,6s
Cert Acquisition Time (PRNn Cert)	960s	480s	192s	960s	192s
Cert Acquisition Time (GALILEO Operator) [12]	840s	420s	168s	840s	168s

Table 8. Performance of NMA using Proposed Scheme - Message Configuration 1

Table 9 details the key performance indicator for message configuration 2, the alternate configuration. It should be noted that this message configuration for the GPS L2C does not comply with the required maximum broadcast intervals. Assuming such a configuration for Galileo, cryptographic integrity can be provided at the integrity performance requirements for time-to-alarm for class B and C applications (Refer to Table 4).

	GPS L2C (25 bps)	GPS L5 (50 bps)	Galileo OS E2-L1-E1$_B$ (125 bps)	Galileo OS E5A$_I$ (25 bps)	Galileo OS E6B$_I$ (125 bps)
Time-To-Alarm (Integrity)	48s	24s	9,6s	48s	9,6s

Table 9. Performance of NMA using Proposed Scheme - Message Configuration 2

Security of the Scheme

In this scheme SHA-1 is used as the secure hash function *F(x)*. The MAC is a SHA-1 HMAC, a MAC based on a keyed hash function. A truncated version of the MAC is transmitted, in which the 78 MSBs of the SHA-1 HMAC computation are transmitted in authentication message type 60.

MAC truncation has both some security advantages and disadvantages, namely that there is less information available to an attacker; however there are fewer bits for an attacker to predict.

It is recommended that a truncated value be at least half the number of bits of the MAC result (80 bits) (Krawczyk et al. 1997), as this is the bound of the birthday attack, and it is a suitably high lower bound for the number of bits an attacker must predict. The truncated value used in the authentication message is 78 bits which is sufficient given that a new hash value is used to key the MAC of a given sequence of messages every timeslot (48/96 seconds). In addition, the validity of the MAC is only one timeslot due to the key being released in the subsequent timeslot, making it computationally infeasible to forge a MAC within this short period.

The EC-DSA public key algorithm is used for distribution and certification of K_0. The elliptic curves used in this scheme are recommended as a secure curve by NIST (NIST 1999).

Archer in (Archer 2002) presents a mechanized correctness proof of the basic TESLA protocol using TAME[13]. Archer concludes that the degree of similarity of the proof of an analogous protocol to the proof of basic TESLA will depend on the degree of difference of this protocol to the basic TESLA. The proposed protocol does not vary significantly from the basic TESLA protocol, except the synchronization of the sender to the receiver.

A security assumption of TESLA is that the sender and receiver remain synchronized. This is critical for the security of the protocol, as a drift in synchronization of the receiver from the sender could result in compromise. Our proposed synchronization system alleviates this issue.

Conclusion

Navigation Message Authentication (NMA) is a good method to provide scalable, security services and anti-spoofing mitigation functionality to the civil community.

We have presented two NMA schemes: a scheme based on digital signatures and a modified version of the TESLA protocol. The proposed TESLA protocol has a number of advantages over the digital-signature approach in terms of computational efficiency, security, flexibility and time-to-alert.

While the proposals were based on the CNAV message structure of the GPS L2C, these authentication concepts can be applied to Galileo as well as Space and Ground-based augmentation systems. While the time-to-alarms of the proposed schemes appear to fulfill requirements for some classes of SoL applications, the actual performance for Galileo will depend heavily on chosen the navigation data structure.

References

Archer, M. "Proving Correction of the Basic TESLA Multicast Stream Authentication Protocol with

[12] Value is based on reception of packets from 6 satellites.

[13] TAME (Timed Automata Modeling Environment) is an interface to PVS, a verification system that supports a specification language integrated with support tools and a theorem prover.

TAME." *Workshop on Issues in the Theory of Security (WITS)*.

ARINC Engineering. (2004). "Navstar Global Positioning System: Interface Specification: Navstar GPS Space Segment/Navigation User Interfaces." GPS Joint Program Office, El Segundo, CA, USA.

Barker, B. C., Betz, J. W., Clark, J. E., Correia, J. T., Gillis, J. T., Lazar, S., Rehborn, K. A., and Straton, H. R. (2000). "Overview of the GPS M Code Signal." MITRE Corporation,.

European Space Agency. (2002). "GALILEO Mission High Level Definition."

Fontana, R. D., Cheung, W., Novak, P. M., and Stansell, T. A. (2001). "The New L2 Civil Signal." GPS World.

Galilei Consortium. (2003). "The Galilei Project: GALILEO Design Consolidation."

Hein, G. W., Godet, J., Issler, J.-L., Martin, J.-C., Erhard, P., Lucas-Rodriguez, R., and Pratt, T. "Status of Galileo Frequency and Signal Design." *Institute of Navigation - GPS 2002*, Portland.

Krawczyk, H., Bellare, M., and Canetti, R. (1997). "HMAC: Keyed-Hashing for Message Authentication." RFC 2104.

NIST. (1999). "Recommended Elliptic Curves for Federal Government Use."

Perrig, A., Canetti, R., Tygar, J. D., and Song, D. (2002). "The TESLA Broadcast Authentication Protocol." *CryptoBytes*, 5(2), 2-13.